10-2017

The Use of Effective Risk Management in Cloud Computing Projects

Usha Kiran Marichetty
Harrisburg University of Science and Technology

The Use of Effective Risk Management in Cloud Computing Projects

Name: Usha Kiran Marichetty

Harrisburg University of Science and Technology

Abstract

Project management is one of the most important procedures that promote delivery of services. Examples of such projects include cloud computing projects. Despite the potential benefits associated with cloud computing projects, there are a number of security risks that when not properly managed, can always lead into the organization suffering major loses. In the adoption of cloud computing systems, project managers should have secure and well-configured platforms to reduce and control risks associated with cloud computing systems. There is a need for adopting the best risk management tools, techniques, and operations to achieve the desired results in the process of adopting cloud computing systems in project management. Risk management main elements include establishing the context, analysing the risks as well as evaluating and monitoring the risks and the communicating such risks to various stakeholders. There is need for integrated risks management to provide proper management, flexible planning as well as recovery plans in case of problems. The top management should always quantify the risks involved and evaluate its major effects on the firm business operations and activities. The present paper aims to achieve its primary objective and purpose by providing a comprehensive review of previous literature related to the use of effective risk management in cloud computing projects. The paper specifically looks at the use of effective risk management in cloud computing projects.

Keywords

Project Management; Cloud Computing and Risk Management

Table of Contents

Contents

INTRODUCTION

1.1 Background information

The dependency that people have on cloud computing is increasing at a high rate as a result of its general cost-effectiveness and some other associated benefits, allowing the organizations to come up with solutions in a very short period of time without wasting too much resources and efforts on the general implementation and instead focuses on strategic objectives. According to recent studies and reports by (Stieninger &Nedbal (2014) however, it is evident that strategic risk management should be incorporated in cloud computing projects. Risk management main elements include establishing the context, analysing the risks as well as evaluating and monitoring the risks and the communicating such risks to various stakeholders. There is need for integrated risks management to provide proper management, flexible planning as well as recovery plans in case of problems. Risk management should also cover loss prevention and other control measures (Stieninger &Nedbal, 2014). This may include loss and risk control through avoidance, through evaluation of problems as well as through risk financing activities. In most cases, risks mainly occur due to failure of the management to adopt effective risk management procedures as well as due to lack of proper decision making framework (Stieninger &Nedbal, 2014). This negatively influences the firm investment activities and might lower achievement of the firm goals. Some of the best procedures that should be adopted in the process of managing risks in the firm include proper and effective collaboration among various stakeholders in the firm (Wang, Wood, Abdul-Rahman & Lee, 2016). Cloud computing projects are highly associated with a number of risk that when not properly managed, can result into major security issues as well as great loss to the company as a whole.

According to Ryan & Buchholtz (2001), companies should always adopt proper procedures to allocate resources to various departments in the firm, have proper risk management mechanism and consider security threats in order to reduce and control security risks that may face them**.** There are some cases where the firm can experience several operational risks in their business operations and such risks should be considered in all the firm operations. It is also true that the firm top management should consider legal risks in their cloud computing projects (Stieninger &Nedbal, 2014). The top management should always quantify the risks involved and evaluate its major effects on the firm business operations and activities (Ryan & Buchholtz, 2001). This is because having the ability to identify risk and absorb it is very critical towards effective risk management and providing informed decision making in the firm.

The need for considering the firm risk appetite is also very important since management risk appetite is part of procedures towards determination of the firm ability to absorb such risks. Through this, the firm is able to adopt the best policies and procedures to eliminate high risks and problems (Ryan & Buchholtz, 2001). However, management should be ready to face all the risk despite their intensity since lack of proper management of risk can lead to low revenue generation, thus preventing the firm from achieving its major goals and objectives.

1.2 Problem Statement and Justification

In the current society, there is a high advancement regarding technology, and many global firms are adopting cloud computing to promote the efficiency of their project management operations. It is also true that the application of cloud computing systems in project management provides secure, affordable and efficient data management and storage (Ferguson-Boucher &Convery, 2011). However, there are various security issues and risks associated with adoption of cloud computing in project management; thus project managers should provide suitable

measures to control and prevent such risks and problems (Wang et al., 2015). It may include the adoption of ethical and legal policies as well as the provision of well-secure and well-configured data management systems. The use and adoption of cloud computing in project management can promote the achievement of the project outcomes and goals (Ryan & Buchholtz, 2001). For security issues and other risks to be properly controlled, understanding the use of effective risk management in cloud computing projects is very important (Lee, 2012).

Risks must always be understood with regards to the whole business opportunity and appropriate measures taken to manage it. Cloud services are never only for convenient storage but also comprise of very important benefits likes convenient communication and collaboration at the multi-point level (Khorshed, Ali & Wasimi, 2012). Hence, the risk involved in cloud computing should always be understood and managed accordingly. It is also possible that the cloud customer can transfer risk to the individual cloud provider and such risk must always be considered against the cost benefit that is obtained from the final services rendered. However, it is important to point out that not all the risks in this case can always be transferred. If a risk result into a business failure, then serious damage to the organizational reputation or legal implications is likely to be witnessed and it becomes very difficult for any other party to compensate for such type of damage (Khorshed, Ali & Wasimi, 2012). This explains why effective risk management in cloud computing projects is very essential to the success of the organization.

Different organizations which handle information security have always done numerous assessments on risk associated with cloud computing and have in many instances generated a number of threats which when not addressed accordingly, can result into great loss in the organization (Khorshed, Ali & Wasimi, 2012). It is also important to highlight the fact that

security breaches is not something new in cloud computing. As a matter of fact, vulnerabilities and threats that had been there within the traditional data centers do also exist in the cloud in a very similar form. One of the great differences that exist between security breaches within the traditional data center and a cloud service is the magnitude of impact when a breach happens to have occurred (Lee, 2012). For instance, two great data breaches that had targeted cloud infrastructure was reported in 2011. These breaches raised great concern regarding cloud security though it also proved that one breach could significantly affect numerous organizations that houses their individual applications and data within the same infrastructure.

This paper specifically looks at the use of effective risk management in cloud computing projects. Literature mentions compliance risks, isolation failure, vendor lock-in, loss of governance, malicious insider, incomplete or insecure data deletion, data protection and management interface comprise as the main risks that are associated to cloud computing. Other genuine threats to cloud computing projects are data loss, malicious insiders, service or account hijacking, issues of shared technology and insecure interfaces (Khorshed, Ali & Wasimi, 2012). Cloud computing are also vulnerable to the risks of data protection, lock-in risk, supply chain failure and network breaks as well as poor network management. Effective management of such risks is very critical for the success of the organization and must always be taken into great consideration (Khorshed, Ali & Wasimi, 2012). In that sense, the present paper aims to achieve its primary objective and purpose by providing a comprehensive review of previous literature related to the use of effective risk management in cloud computing projects. The literature review findings and results will contribute to future research references on the same topic. In the process of evaluating and providing a systematic literature review to investigate the use of effective risk management in Cloud Computing Projects, the paper will also incorporate practical

approaches and examples to security issues. However, the fact that not many studies have been done on the use of effective risk management in cloud computing projects makes this present research very necessary.

The broad objective of this study is to determine the main risks associated with cloud computing projects and the use of effective risk management in such cloud computing projects. Based on this broader objective, this study seeks to fulfil the following specific objectives:

1. To investigate main risks associated with cloud computing projects
2. To establish the use of effective risk management in cloud computing projects

The only limitation of this research is based on the fact that it will mainly rely on systematic review of literature instead of using primary data such as interviews and questionnaires in investigating how effective risk management can be used in cloud computing.

LITERATURE REVIEW

2.1 Security risks in cloud computing projects

It is worth noting that cloud computing systems have broad network access especially due to the application of standard mechanism in their network operations (Ray, 2016). It is evident in several applications such as in mobile phones and laptops where people involve the use of broad network access systems (Royston, 2016). Moreover, cloud computing systems also include resource pooling to serve different clients in the society (Zimara, 2013). In most cases, cloud computing systems include multiple tenant model systems and other virtual resource applications (Ray, 2016). These resources promote data storage, processing as well as network access systems through the use of virtual machines and emailing systems (Zimara, 2013). Through its resource pooling characteristics, cloud computing systems can also promote economies of scale in global firm operations and activities (Royston, 2016). There are also those who argue that cloud computing systems include rapid elasticity characteristics at different times and locations (Ray, 2016). Also, cloud computing systems are measured and can be controlled as well as in particular through the application of transparent and consumer based services delivery systems (Ray, 2016). In that sense, global project managers could ensure that their cloud computing applications meet the resource and the firm budget plan (Royston, 2016). Project managers should understand the higher one uses the cloud computing systems, the higher the bill. Cloud computing systems are part of network security management systems that global firms use to sell their voice and data services (Ray, 2016). Consequently, cloud computing systems are also policy driven and are well isolated and segmented as well (Zimara, 2013). It provides good governance and the flexibility of services delivered through cloud computing systems (Royston, 2016).

Despite this however, literature reports several security risks that are associated with cloud computing. Most of such risks are full dependent on the cloud service provider. As had been reported in the case of FBI raid in Texas, in the event that the provider becomes inoperative, either involuntarily or voluntarily, then the agencies are most likely to suffer great loss of data and service they are offering (Zissis & Lekkas, 2012). For such catastrophe to always be avoided, then proper mitigation and assessment of security risks must always be put in place. Having full dependency on the security assurance of the service provider as well as other practices is another concern of security risk. It is important to note in the first place that inadequate security controls of the provider of cloud service can always jeopardize the general integrity, confidentiality and presence of information from the agency (Zissis & Lekkas, 2012). Moreover, ceding control to the provider of cloud service can always result into great loss of governance and the physical control over information and proprietary data.

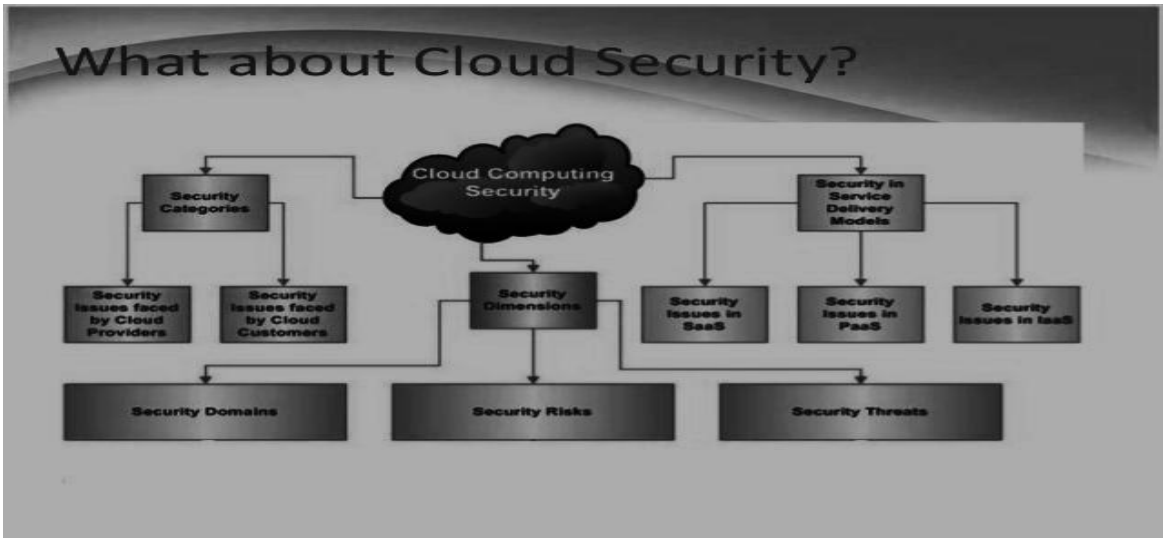


Figure 1: Cloud security (Zissis & Lekkas, 2012)

Malicious and wrongful activities by the individual employees from the service providers can as well result into leakage and loss of important data (Zissis & Lekkas, 2012). All these

risks are however not specific to a given cloud computing project and must always be managed more effectively for successful results to be realized. In order to mitigate such risks, string controls internally must always be put in place, especially with very strict segregation of the individual duties, monitoring, access control management and independent auditing. Such factors must always be investigated very carefully and evaluated during the process of selecting service provider (Chen & Zhao, 2012). The other security concern of a number of organizations has always been sharing of computer resources by many organizations. Within a virtualized environment in which numerous virtual servers are all hosted within one physical host computer, there exist a risk for access privileges to some other virtual machine to be offered in error, leading to a loss in the confidentiality in data and most likely an exposure to relevant information (Chen & Zhao, 2012).

Figure 1—Ranking Comparison of Top Risks

Risk	CSA Ranking	OWASP Ranking	ENISA Ranking
Abuse and nefarious use of cloud computing—Due to the often anonymous nature of some cloud services, they attract use by criminal elements.	1	-	-
Insecure interfaces and application programming interfaces (APIs)—Due to the open nature of cloud services, interfaces and APIs often use anonymous access, cleartext authentication or content transmission.	2	-	-
Malicious insiders—Cloud providers offer little transparency into their supply chain, human resources, security management or incident management processes.	3	-	8
Share technology (multitenancy/isolation) risk—One tenant can deliberately or inadvertently interface with the security or performance of another tenant.	4	7	3
Data ownership (governance) and accountability—Data ownership, encryption, transmission, operational failure, data disposal/data deletion and availability are all challenges in a cloud environment.	5	1 (Ownership) 5 (Data loss)	1 (Ownership) 7 (Data deletion)
Account or service hijacking (including management interface)—Using social engineering, phishing, fraud or vulnerability exploits, attackers can compromise confidentiality, integrity and availability.	6	9	5
Unknown risk profile—Cloud providers offer little transparency into compliance, security procedures, configuration management, logging and monitoring, leaving customers with an unknown risk profile.	7	8	-
User identity federation—Use of multiple cloud offerings can result in islands of identities that need to be maintained.	-	2	-
Regulatory compliance—Regulatory environments differ across countries and regions, particularly with regard to privacy.	-	3	4
Business continuity and resilience—These are delegated to the cloud provider and may not be appropriate. Pricing pressure results in commoditisation that de-emphasises this.	-	4	-
Service and data integration/protection—Data handling or data protection fails during transmission between end user and data centre, or between federated clouds.	5 (CSA covers both this risk and the other data risk noted previously.)	6	6
Non-production environment exposure—A cloud provider is used for design, development and test activities, which are typically less controlled.	-	10	-
Lock in—Minimal tools, procedures, standards or interfaces are in place to guarantee data, application, service or business process portability.	-	-	2

Figure 1: Risks involved in cloud computing projects (Chen & Zhao, 2012).

In order for one to mitigate such kind of risks, strong internal understanding and control is needed. To be specific, there is need for formal authorization procedure for access control to be enforced after being established. Moreover, each and every activity and access need to be logged, with the access control matrix being reviewed after some period by auditors who are independent (Khorshed, Ali & Wasimi, 2012). Literature always refers to independent auditors who do periodic assessment of privacy impact, security controls as well as performance as cloud auditors. Cloud auditors are party that is capable of conducting independent assessment of different cloud services, security of the cloud implementation and information system operations (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Näslund & Pourzandi, 2012). Auditing done by both external and independent party is a very important process for the federal agencies since such agencies that employ cloud computing model within the infrastructure of their information technology usually include a contractual clause that enables the third party to get access to security control of all the cloud providers. It is very much unfortunate that most of the scholarly works have failed to capture the aspects of internal controls (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Näslund & Pourzandi, 2012). Proper risk management strategies must be put in place for the purpose of internal control in areas such as change management, maintenance, system security and configuration management.

In the current society, many global firms include rules and policies that regulate their governance systems (DavoudJolfaie et al., 2015). The rules adopted prevent and control loss of their critical data and improve the reliability of the cloud computing procedures and applications (DavoudJolfaie et al., 2015). There are also firms that include data encryption methods to prevent and control security problems in their cloud computing applications (Charlebois, Palmour&Knoppers, 2016).

Therefore, it is true that global firm's managers can use cloud computing platforms to store their data over the internet (Charlebois, Palmour&Knoppers, 2016). Despite this, there are some negative consequences associated with cloud computer applications in project management. For example, there are those who argue that cloud computing may experience some security problems (Charlebois, Palmour&Knoppers, 2016). For example, where are cases where global firms face intellectual property and copyright problems towards their information stored in cloud computing platforms (DavoudJolfaie et al., 2015). It is also true that global firms who use cloud computing systems in their project management experience limited customized options on their data (DavoudJolfaie et al., 2015). However, it should be noted that cloud computing application provides high economies of scale and it is also cost effective compared to other project management applications (Charlebois, Palmour&Knoppers, 2016).

With the current advancement of technology, it is important that global project managers adopt secure and well-configured cloud computing systems in their project management activities. It is true that cloud computing applications promote efficiency; cost efficient and quality of services in project management (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Näslund & Pourzandi, 2012).Therefore, global firms should aim at using virtual networks systems to improve their data management and have a good relationship with their employees.

The application of well secure cloud computing systems will increase trust and confidence in all project management activities (Singh, &Chana, 2015). To reduce and control security issues and risks associated with cloud computing applications in project management, global project managers should adopt the use of secure passwords and other authorization systems to promote the intellectual rights of their data stored on cloud computing systems (Shahzad, Golamdin& Ismail, 2016). There is also the need for using hybrid cloud computing

models which cover both private and public cloud computing systems (Nicoletti, 2012). It is also important that global project managers aim at adopting affordable, scalable and secure cloud computing systems. Cloud computing systems adopted by global firms should also meet the legal procedures and standards (Gonzalez & Smith Jr., 2014).

The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. This can be considered especially important in the case of cloud computing due to the fact that cloud architectures necessitate certain roles which are extremely high-risk (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Näslund & Pourzandi, 2012). Examples of such roles include CP system administrators and auditors and managed security service providers dealing with intrusion detection reports and incident response. As cloud use increases, employees of cloud providers increasingly become targets for criminal gangs (as has been witnessed in the financial services industry with call centre workers) (Khorshed, Ali & Wasimi, 2012).

2.2 Risk management in cloud computing project

Han (2011) argues that there are various risks and problems associated with cloud computing applications in project management. For example, cloud computing promotes CSP incompatibility problems, increase privacy and confidentially control problems and may also lead to the firm poor data integrity systems (Han, 2011). Project managers adopt the use of secure architecture, in controlling service delivery systems during project management with cloud computing (Bildosola et al., 2015). It may include the adoption of fiber optic connectivity as well as other environmental friendly cloud computing systems (Han, 2011).

There are some success factors that global firms should consider in the process of risk management in their project management activities (Stieninger&Nedbal, 2014). For example, cloud computing promotes and increase trusted relationship between the management and the firm clients (Stieninger&Nedbal, 2014). In that sense, cloud computing applications and activities can promote IT familiarization and improved the economies of scale in global firms (Stieninger&Nedbal, 2014). Adopting cloud computing practices in project management operations should include security issues (Backe& Linden, 2015). Some of the security issues identified include multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, loss of monitoring and availability, as well as trust management (Backe& Linden, 2015). Security solutions identified include security models, auditing, policies, SecCloud, RAID, biometrics, self-destructing data, and service hardware when the virtual or physical hardware is needed (Backe& Linden, 2015).

In the process of promoting their project management activities and operations, global project managers should consider effective management of risk that are related to cloud computing (Bildosola et al., 2015). Providing security controls and adoption of the risk management strategies can promote successful application of cloud computing in project management activities and operations (Backe and Linden, 2015). According to studies and publications by Backe and Linden (2015), the majority of security problems in the Cloud Computing have been theoretical therefore there is a need for the promotion and adoption of practical approach towards security issues and their solutions in the Cloud Computing (Backe and Linden, 2015). This can only be realized when there is proper strategy put in place for effective risk management.

Furthermore, a literature review by Backe and Linden (2015), suggested that all the security issues and solutions are relevant to the field of project management as long as it involves the application of Cloud Computing (Backe and Linden, 2015). According to Bildosola et al., (2015), information technology forms one of the best practices that have led to proper cloud computing operations and systems (Bildosola et al., 2015). Through the application and use of cloud computing activities global firms are currently able to add value to their project management activities including their information handling and storage applications. It is mainly because cloud computing applications mostly revolve around the remote and virtual management systems and may help global firms to save their management costs to great and complex projects (Bildosola et al., 2015).

METHODOLOGY

3.1 Introduction

This chapter provides a deep explanation of the study design applied in the whole process of data collection. Some other aspects included comprise of sample size determination and sampling techniques, data collection, data analysis, validity and reliability, and lastly ethical considerations.

3.2 Purpose of this survey

In order to help solve the problem of risk management in cloud computing projects, the researcher intend to seek for the opinions and perceptions of software engineers who are familiar with cloud computing so that great solutions can be generated in relation to managing risks in cloud computing. Previous studies have always mentioned the existence of a number of risks in cloud computing without giving solutions onto how such risks can properly be managed. That is the gap this study seek to fill, by highlighting each and every risk associated with cloud computing and the corresponding solution to each risk. Moreover, the present paper aims to solve the problem by providing a comprehensive review of previous literature related to the use of effective risk management in cloud computing projects. It seek to use both primary and secondary data in the methodology so as to provide comprehensive solution to the aspect of risk management in cloud computing.

3.3 Study design

This study aimed at utilizing cross-sectional study design within which data has been collected via quantitative and qualitative methods. Literature defines cross-sectional study design as that one which comprise of either doing a study to whole group of people or taking a sample that is representative to the whole population (Gysels, et al., 2013). It comprise of making a

snapshot of a study, doing a study only at one specific point in time without some major follow-ups. The study is referred to as cross-sectional because it was carried out only at one point in time without a repeat of the same (Wilson, 2013).

Quantitative study is defined as one which involves counting of things, analysis of data involves statistical methods and the generated results are quoted in a numerical form. Approaches that are involved in the quantitative research methodology usually comprise of experimental research, descriptive studies and quasi-experimental studies (Creswell, 2013). Moreover, research which is quantitative in nature always aims at offering relevant predictions and explanation of generalized findings. The focus in such circumstances is to make a confirmation or rather validation of the already existing relationships and generate generalization that can be used in the in developing a number of important theories (Gysels, et al., 2013). Quantitative method in this research seeks to quantify and categorize the main risks associated with cloud computing projects and establish the use of effective risk management in cloud computing projects. It is important to note that the researcher aim at establishing the main risks associated with cloud computing projects and how to effectively manage such risks. These risks can only be established through quantitative study where quantitative data are obtained from the people who have experience with the concept of cloud computing. It can help give the answer in numbers, illustrating the main cause with regards to numerical strength.

As per the illustration from McCusker & Gunaydin (2014), qualitative research comprise of doing a review on the individual characteristics or qualities that cannot be presented in numerical value. It is a kind of study that has its main focus on the occurrences that occurs within natural settings and includes doing a study of such kind of phenomena within all the complexity (Cochrane Handbook for Systematic Reviews of Interventions, 2008). In the same

context of this present study, scholars have offered a number of suggestions that both structured and systematic approaches are very important in handling the issues to do with risks associated with cloud computing. Questions such as what you think are the main risks associated with cloud computing can never be quantitative but can only be in the qualitative form so that answer can be generated very easily (Cochrane Handbook for Systematic Reviews of Interventions, 2008).

Qualitative methodology was used in the study for the purpose of getting to understand the actual risks associated with cloud computing and how such risks can effectively be managed (Gysels, et al., 2013). Scholarly literatures show that qualitative study is usually exploratory in their individual natures and might comprise of interviews or desktop research (Wilson, 2013).

Qualitative paradigm has been picked for this study due to the reason that qualitative research always describes and narrate the experience of individuals prior to making a meaningful conclusion from it. Applying qualitative method of data collection has offered the researcher with the great chance of investigating main risks associated with cloud computing projects and the use of effective risk management in such cloud computing projects (Cochrane Handbook for Systematic Reviews of Interventions, 2008). As stated by the scholars, qualitative study provides the researcher with essential opportunity of having a focus on the problem with some greater depth through application of different lenses (Watzlawik & Born, 2007). Based on the fact that this study has its emphasis on the best way to handle risks related to cloud computing, following an approach which appears naturalistic would assist the researcher to answer the research question by giving him the chance of doing assessment on best way to do the same (Watzlawik & Born, 2007). Methods like using interview questions allowed the researcher to get to understand the voice of the participants on the manner in which they share their individual opinions about the best way to minimize risks and cloud computing projects.

The other explanation on why qualitative paradigm had been chosen for this study is as explained by Yin (2013), qualitative studies usually have their focus on the general meanings and experience that people develop from their own forms of experiences. That is to say, getting to understand the meaning of a given individual usually arise through investigative methods on her beliefs and perceptions and this help provide reflection of their individual actions and behaviours (Gysels, et al., 2013). In respect to that, it has been found very crucial to understand the perceptions of students regarding the main risks associated with cloud computing and how to effectively manage such risks in cloud computing projects.

Using interviews with the key informants like software engineers would provide the researcher with enough opportunity to get detailed information from the respondents without any form of limitation on what to say and what not to say (Cochrane Handbook for Systematic Reviews of Interventions, 2008). In that essence, the researcher is entitled for the best possible results so as to help answer the intended research question.

3.4 Method of data collection

As had been mentioned, both quantitative and qualitative data have been collected for the purpose of answering research questions in this study. While the quantitative data has been collected by administering questionnaire to software engineers working in various departments in the country, both systematic review of literature and open ended questions will be used for the purpose of collecting qualitative data (Gysels, et al., 2013). The main instrument used in this study for the purpose of data collection is a 15 item questionnaire. The other instrument which is worth mentioning is the secondary literatures which has been used both at the literature review section as well as in getting deeper findings regarding the risk associated with cloud computing and the best way to manage such risks. It is important to note that the questionnaires will be sent

to the software engineers who the research is acquainted to and asked to give their views and perceptions via emails. The study utilized both open-ended questions and multiple choices questions in the questionnaire. The open ended questions had been assumed fit for the purpose of this study as it gave the respondents the freedom of answering the questions in the best manner and wordings they feel like using, without restricting them to the possible choices of answers. This could generate answers which are more detailed for the purpose of analysis and discussion. Moreover, the researcher also made use of multiple choices questions, thanks to the fact that they are cheap and easy to be analysed. In the multiple choices questions, the respondent is expected to provide finite answers from a number of choices they are provided with and hence is limited with options of trying to figure around with words. They are left with specific answers to choose from. Multiple choices questions are usually batter than the open ended questions which require some additional analysis by the researcher for them to generate any meaningful findings and hence both time consuming as well as very expensive (Caillaud, Rose & Goepp, 2016). This offers an explanation why the researcher entirely relied on multiple-choices question system with very limited number of open-ended questions (Caillaud, Rose & Goepp, 2016).

The questionnaire in this case had different sections, with the first section containing general information related to gender, age, and marital status of the respondents while the second section contained questions pertaining to potential risks associated with cloud computing projects and lastly, the third section of the questionnaire contained questions pertaining to effective strategies for managing risks associated to cloud computing.

The study also considered secondary literature as the researcher aimed at obtaining a variety of scholarly views on how risk can properly be managed in cloud computing project.

Research review will not be limited to a particular theory so long as the source of material emphasizes on qualitative research based on the topic (Gysels, Evans, Lewis, P, Speck, Benalia, Preston, Grande, Short, Owen-Jones, Todd & Higginson, 2013). It is hoped that with the utilization of this methodology together with others, a comprehensive analysis of the usage of effective risk management in cloud computing projects could done.

Key words such as risk management and cloud computing were entered into computer system and a search done to generate scholarly articles on the topic of using effective risk management in cloud computing projects. These key words were entered in computer databases such as Google scholar, Ebscohost, among other databases and relevant articles generated for analysis and discussion. Though the strategy of the search did focus mainly on academic journals, other materials like government reports and data bases were also be utilized for the purpose of systematic literature reviews part of this study (Wilson, 2013). Books were also used in this study mainly for the purpose of meanings definition, and description of the aspects of risk management within cloud computing projects (Gysels, Evans, Lewis, P, Speck, Benalia, Preston, Grande, Short, Owen-Jones, Todd & Higginson, 2013). It was assumed that such books and journals would present an exhaustive literature review on the kind of risks involved in cloud computing and how such risks can best be managed. It is important to note that only articles and journals that are updated, not more than 7 years old since the date of publishing, written in proper English and have the required content as per the study topic have been included in the study (Wilson, 2013). This ensured that reliability and validity of the study is assured. Up to 25 secondary journals and scholarly articles have been included in the study.

3.5 Validity of study instruments

Validity and reliability are basic cornerstones of research as they are construed as proofs for scientific/systematic research processes. Reliability implies the repeatability/consistency of findings when similar procedures are followed. For instance, if the study were to be undertaken again, the results should be the same (Caillaud, Rose & Goepp, 2016). On the other hand, validity implies the credibility or believability of the study. Validity can be viewed through two aspects; internal validity requires that the instruments/tools or procedures applied in the research measured what they were intended to measure. While external validity is concerned with generalization of findings beyond the immediate study (Creswell, 2013).

In this context, reliability and validity was addressed by developing systematic, appropriate and logical research design from the research approach, research methods, population sampling, data collection methods, data gathering tools/instruments, and accurate analysis/interpretation and inference of the findings (Caillaud, Rose & Goepp, 2016). The researcher did undertake a reconnaissance study, prepared sample research instruments, for instance, questionnaires for pre-testing study which enabled researcher to correct discovered errors before the actual field work.

That is for instance, questionnaires questions were never ambiguous and started with simple questions, in-depth literature review and expertise consultations was also done, sizeable samples determined to ascertain representativeness, diverseness, and successful generalization of the results (Caillaud, Rose & Goepp, 2016).

3.6 Targeted population and sampling method

For the purpose of answering the research questions, the targeted population in this study was software engineers working for different organizations within the country. Software engineers working for different firms in the country formed the sampling frame for the study out of which 15 were chosen as research participants using non-probability sampling techniques.

With regards to non-probability sampling technique, there is no chance of making sure that all the potential population have equal chance of participating in the study. Participants were chosen to take part on the study based on the fact that the researcher was acquainted to them and could reach out to them via email (Caillaud, Rose & Goepp, 2016). This kind of sampling method is commonly described as purposive sampling, in which individuals are picked to take part in the study due to some specific reasons (Cochrane Handbook for Systematic Reviews of Interventions, 2008). This type of sampling technique is very essential, more also when the population being studied is somehow small in size (Gysels, et al., 2013). The researcher is not very familiar with most software engineers throughout the country, a factor that confirms the need for purposive sampling, selecting the software engineers to participate in the study as long as she/he meets the following inclusion criterions: Has job experience in matters related to cloud computing is working in organization that has implemented cloud computing projects at their places of work and understand the major risks that are associated with cloud computing projects.

3.7 Data collection procedure

The process of data collection involved administering questionnaires to numerous software engineers working in different organizations within the country. The research first reached out to the potential perticipants via phone, asking them if they could agree to take part in the study. They were asked for their consent and willingness to take part. The aim of the study

was first explained to each individual (Doorn, 2010). The researcher also explained to the participants how the study could benefit them hence the need of them to participate and express their opinions and experience. Upon agreeing to be part of the stud, the researcher requested for their mails and sends them questionnaires to be filled in one week and sent back via mail (Doorn, 2010). A total of 15 questionnaires were sent to software engineers who the research managed to reach out and accepted to be part of the study participants.

3.8 Data analysis

Evidence collected from qualitative research and that collected from quantitative research were brought together. At this stage, the researcher utilized deductivist and interpretivist approaches to make meaning and connection between qualitative and quantitative evidence (Bendixen & Yurova, 2012). Quantitative data were entered into a computer system with SPSS software and analyzed accordingly. The data from the analysis have been presented in forms of tables and figures. The numerous risk associated with cloud computing were generated for that matter and the effective strategies to manage each risk suggested by the respondents (Bendixen & Yurova, 2012). Qualitative data on the other hand were run through word-processed format with some sizable margin left on either side. The data collected was then coded by applying circling chunks, writing some specific word that would give category within the margin and applying different highlighter colours to differentiate themes. This was continuously done so as to come up with strong categories and matching the relevant themes with proper codes that would support it.

With sufficient qualitative evidence backing the empirical evidence found from the quantitative research, the researcher then moved to make worthwhile conclusions that sufficiently answered the research questions and confirmed the fulfillment of the research

objectives as outlined earlier in the paper. Information that was collected from 25 journal articles were also retrieved, recorded and summarized. The information was then coded and grouped accordingly into important themes for further analysis and interpretation.

3.9 Ethical considerations

It is important to point out that ethical requirements will be followed to the later. To begin with, the researcher first sought for permission from the university prior to beginning the actual study. The study only started after the university had given out ethical clearance certificate based on the topic of the study (Adhariani, Sciulli and Clift, 2017). Before an individual took part in the study, they were properly briefed regarding the research objectives and the fact that this study does not yield any potential harm to them. This was done prior to administering the questionnaires to them via emails (Caillaud, Rose & Goepp, 2016). Participants were given chance to participate in the study only after giving their individual informed consent via email (Adhariani, Sciulli and Clift, 2017).

Based on the fact that the study also involved review of secondary data, especially from books, academic journals and articles, authors of these literatures were acknowledged through in text citation and referencing for conformity to plagiarism policy. Gathering of information from such documents was conducted using a systematic review design with the utmost integrity and responsibility and at the same time avoiding any form related to misconduct (Wisdom, Cavaleri, Onwuegbuzie & Green, 2012). The analysis and synthesis of other people's ideas was done in a manner that respect the copyright related regulations on the primary sources; presenting a work which has been plagiarized and is having redundant duplications, contravening public guidelines and ethics, and borrowing data from reports which have insufficient ethical standards (Wisdom, Cavaleri, Onwuegbuzie & Green, 2012). Last but not least, all the information generated from

systematic review of literature have been coded and grouped accordingly into important themes for further analysis and interpretation.

FINDINGS AND ANALYSIS

4.1 Introduction

This chapter provides a deep analysis of the study findings and results from the survey monkey in attempt to answer the two research questions: the main risks associated with cloud computing projects, and the use of effective risk management in cloud computing projects.

4.1 Demographic variables

What is your Age bracket

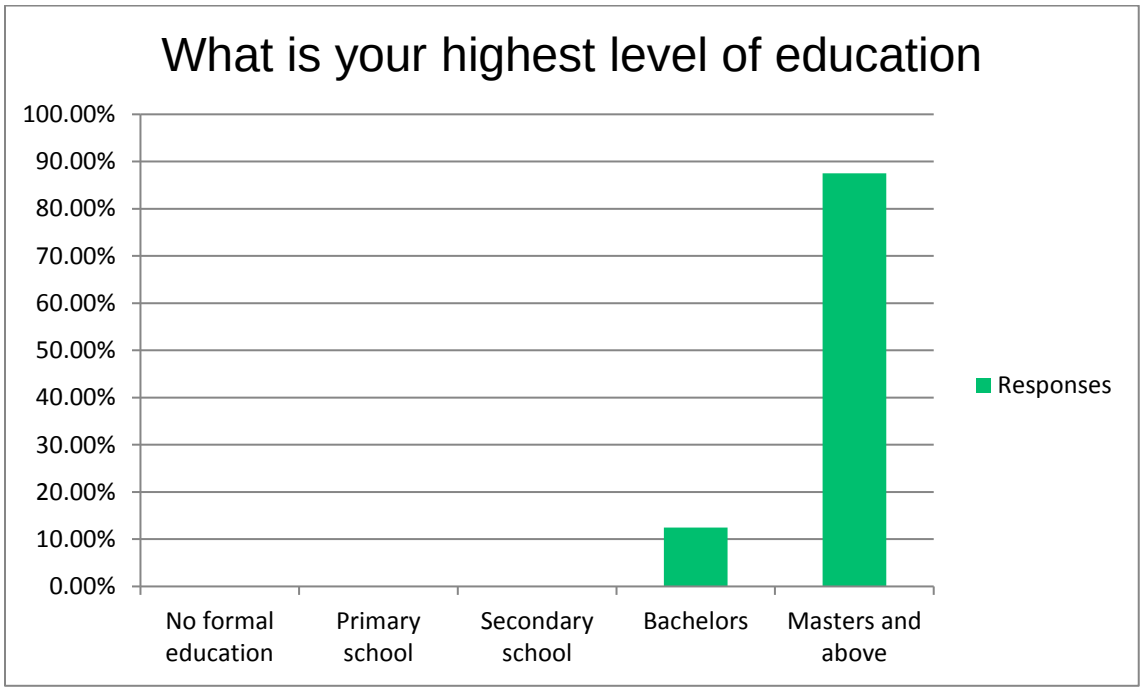
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	(18-23)	0	0	0	0
	(24-29)	3	37.5	37.5	37.5
	(30-35)	3	37.5	37.5	75
	(36-41)	2	25	25	100.0
	Total	8	100.0	100.0	

Only 8 people responded to this question. The above table shows that the age bracket of 18-23 is of 0 individuals, percentage is 0, valid percentage is 0 and cumulative percentage is also 0. The age bracket of 24 to 29 is of 3 individuals, percentage is 37.5, valid percentage is 37.5 and cumulative percentage is also 37.5. The age bracket of 30-35 is of 3 individuals, percentage is 37.5, valid percentage is 37.5 and cumulative percentage is also 75. The age bracket of 36 to 41 is of 2 individuals, percentage is 25, valid percentage is 25 and cumulative percentage is also 100. The majority of the respondents however, felt under the age bracket of 24 years to 30 years old.

Respondents were asked to state their highest level of education. 87.5% of all the respondents stated that they had masters and above, 12.5% had bachelor degrees while none of the respondents had primary, secondary or no formal education levels. The figures are as illustrated in the table below.

What is your highest level of education

Answer Choices	Responses	
No formal education	0.00%	0
Primary school	0.00%	0
Secondary school	0.00%	0
Bachelors	12.50%	1
Masters and above	87.50%	7



Asked about the role each plays in the company, several responses were received ranging from support engineer, administrator, developer, not working, head of Integrated Computer Technology procurement department, assistant director for Information System Department, Software Engeneer, and takeover manager.

4.2 Security Risks in Cloud Computing Projects

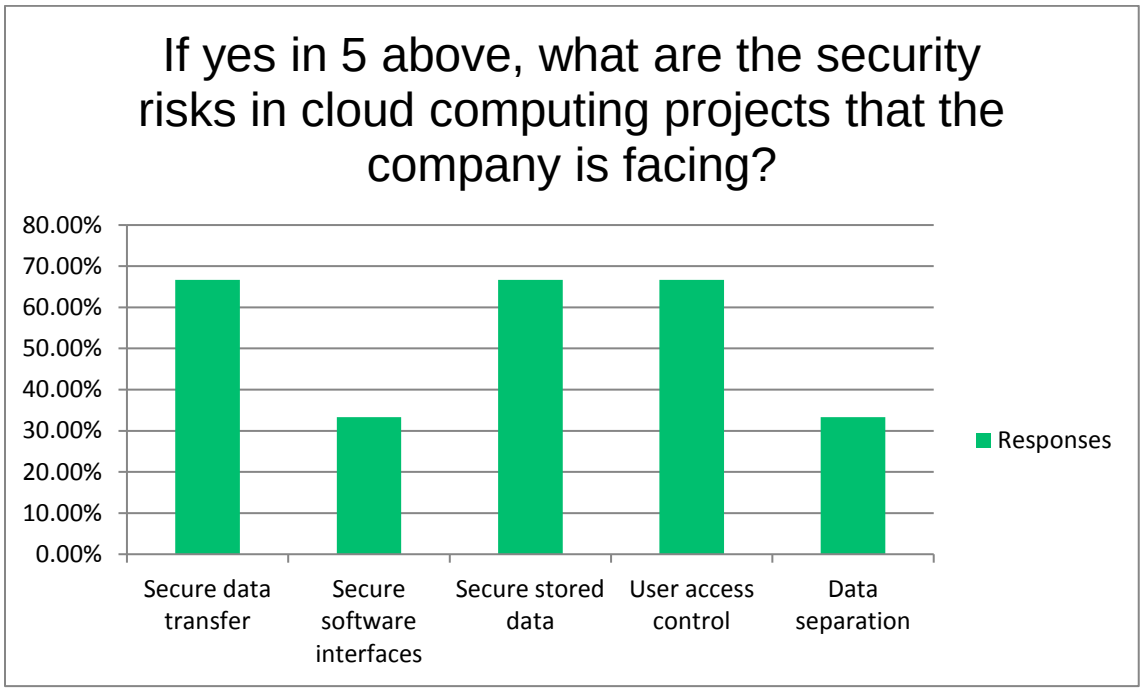
It was very clear from the respondents that the company implement cloud computing with 87.5% of the respondents stating "Yes" while only 12.5% stated "No". A summary of these responses are illustrated in the table below.

Does your organization implement Cloud Computing Projects?			
Answer Choices	Responses		
Yes	87.50%	7	
No	12.50%	1	

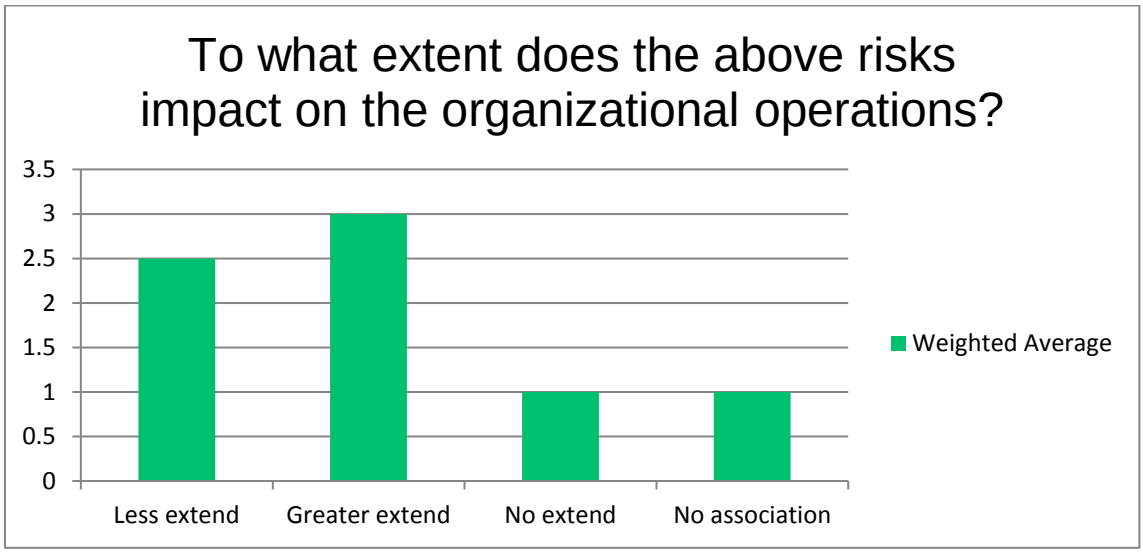
Asked to state if the company experiences security risks in their cloud computing projects, three-quarters of the respondents stated Yes while only 25% of the respondents stated No. Those who stated "Yes" clarified further that the main security risks being experienced at the company are related to data separation, user access control, secure stored data, secure software interfaces, and secure data transfer. A summary of these two responses are illustrated in the table and figure below:

Does your organization experience any security risks in its Cloud Computing Projects?	
Answer Choices	Responses

Yes	75.00%	6
No	25.00%	2



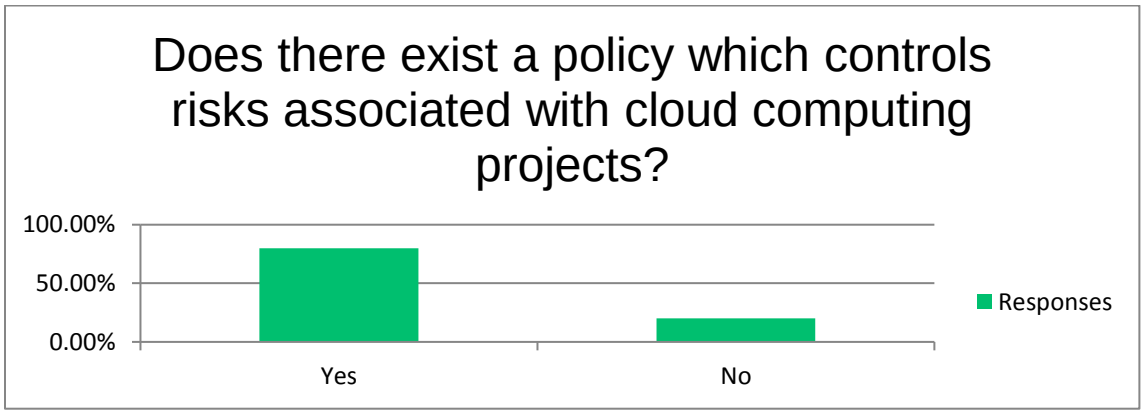
Asked to state the extent to which the above risk impact on the operation of the organization, the average weighted score was 2.5 (less extends) though a larger proportion of the respondents were categorical that the above risks significantly impact on their operations. Still, some few number of the respondents stated that the risks they experience at the company only impact on their operation in some smaller way or in no way at all. A summary of these responses are shown in the figure below.



The respondents were also categorical that the administration are very serious about the risks associated with cloud computing projects in their companies and are doing all that it takes to correct such occurrences.

4.3 Effective Risk Management in Cloud Computing Projects

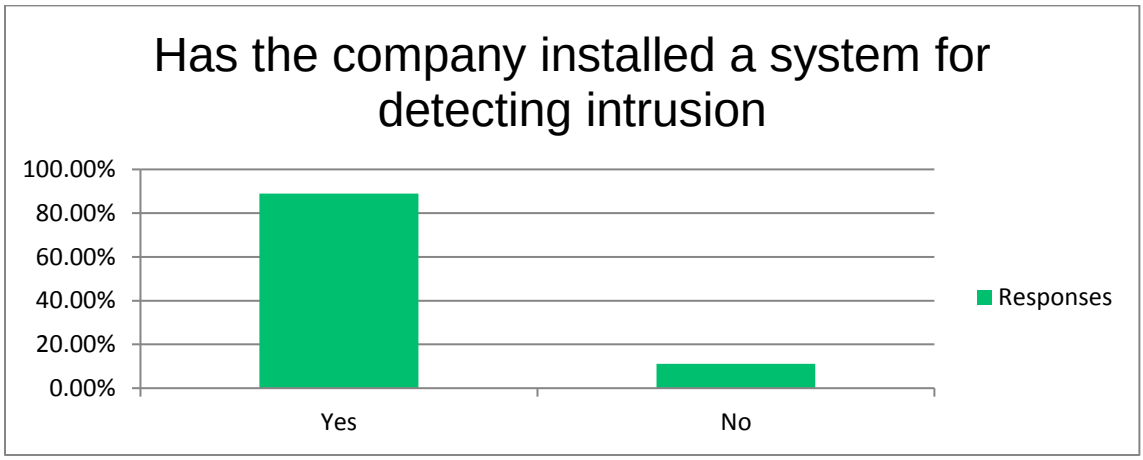
The respondents demonstrated that there exist a number of policies in the company that is used in the management and control of risks associated with cloud computing projects. The responses from this question are as illustrated in the figure below:



Asked to state if the organization have proper system for management of multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, loss of monitoring and availability, as well as trust management, close to 90% of the respondents stated “Yes” while only 10% stated “No”.

Does the organization have the proper system for management of multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, loss of monitoring and availability, as well as trust management?		
Answer Choices	Responses	
Yes	88.89%	8
No	11.11%	1
	Answered	9
	Skipped	1

The respondents also stated that they always block/monitor unproductive website browsing. 67% of the respondents affirmed that they always monitor/block unproductive website browsing while another 33% of the study participants stated that they never block nor monitor any form of unproductive browsing in their websites. Moreover, 100% of the respondents stated that the company has corporate anti-virus software; 89% of all the perticipants stating that their companies have installed a system for detecting intrusion. Respondents also stated that their companies have installed firewall for preventing and controlling all forms of malicious attacks. The statistics are illustrated in the figure below:



The antivirus software in this case was reported to be protecting the servers, PCs, Gateways, plus some other things which are vulnerable to attack by malicious users.

Asked to explain how the installed system is effective in managing risks associated to cloud computing projects in the company, several responses were received. One of the respondents stated, “We have a very well managed infrastructure which will constantly monitor the systems”. “The installed system would create the privacy and security both from insiders and third parties of the organization,” another respondent explained. Some other respondents stated that the security team always monitor all the outside hackers or other ways of people or links trying to enter their domain and block them as well as making sure they have a strong secure network with good privacy policies. The forth respondent was categorical when he clarified that they detects unpermitted intruders who pose risks to the organization and they also rapidly develop and deploy innovative cloud-native applications designed for the cloud economy. Other groups of respondents stated that they always prevent unauthorized access through a security team that monitors all the outside hackers or other ways of people or links trying to enter their domain and block them as well as making sure that they have a strong secure network with good privacy policies.

As the company continues to implement effective risk management in cloud computing projects, it was reported by the respondents that they always face a number of barriers. The barriers in this case include lack of experienced team, unexpected threats and budget issues as explained by one of the respondents "unavailability of well experienced team everyday new threats coming up in the market maintenance of servers budget." The respondents also clarified that they always experience recurrent software attacks by viruses introduced by employees connecting gadgets to company computers. Other barriers commonly mentioned by the respondents were lack of knowledge, issues of deployment, inefficiency to carry out regular updates of antivirus, and constant change of IT setup based on the requirements of the business.

The respondents recommended a number of actions that the organization need to do in order to ensure effective risk management in cloud computing projects. The recommended actions in this case comprised of strategic planning and execution of the plan, regular backups and restoration mechanism, continuous updates of software and antivirus to avoid the system patches, taking the necessary steps to secure the data and servers available in the company domain, ensuring the security features are up to date to be effective in preventing attacks by malware, having strong Management and problem solving skills, ensuring the security features are up to date to be effective in preventing attacks by malware, investing more on the security of the cloud computing systems, and lastly, taking necessary steps to secure the data and servers available in the company domain.

DISCUSSION

5.1 Introduction

This chapter presents a discussion of the study findings and results, making comparison with literature review for the purpose of answering the two research questions: the main risks associated with cloud computing projects, and the use of effective risk management in cloud computing projects.

5.2 Main risks associated with cloud computing projects

It was evident from the respondents that most companies have always implemented cloud computing projects in their operations. While the aim of such projects has always been to improve the general efficiency and effectiveness of the company operations, there are a number of security risks associated with cloud computing projects. The study respondent stated that cloud computing projects come with a number of security risks that always need to be mitigated. Perticipants stated that the main security risks being experienced by companies are related to data separation, user access control, secure stored data, secure software interfaces, and secure data transfer.

This confirms the report from the literature review that had indicated that there are several security risks that are associated with cloud computing. Literature identified most of such risks as fully dependent on the cloud service provider. As had been reported in the case of FBI raid in Texas by Zissis & Lekkas (2012), in the event that the provider becomes inoperative, either involuntarily or voluntarily, then the agencies are most likely to suffer great loss of data and service they are offering. Malicious and wrongful activities by the individual employees from the service providers can as well result into leakage and loss of important data (Zissis & Lekkas, 2012). These risks are however, as reported by the respondents as well as literature

review, not specific to a given cloud computing project and must always be managed more effectively for successful results to be realized. The other security concern pointed out by both the respondents and the literature review is that associated with sharing of computer resources by many organizations. Literature had reported that within a virtualized environment in which numerous virtual servers are all hosted within one physical host computer, there exist a risk for access privileges to some other virtual machine to be offered in error, leading to a loss in the confidentiality in data and most likely an exposure to relevant information (Chen & Zhao, 2012). This was also confirmed by the respondents when they stated that sharing of computer resources by different users always threaten the security and confidentiality of data generated by such computer resources.

The respondents stated that security risks associated with cloud computing always impact severely on the operation of the company as it results into loss of data, finance and important information including company resources. A larger proportion of the respondents were categorical that the above risks significantly impact on their operations. This affirms the argument by Khorshed, Ali & Wasimi (2012) who stated that malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees. Moreover, as the use of cloud computing continues, the employees of cloud providers increasingly become targets for criminal gangs (Khorshed, Ali & Wasimi, 2012). Despite all these, it was evident from both the respondents and literature review that company administration are always very serious about the risks associated with cloud computing projects in their companies and are doing all that it takes to correct such occurrences.

5.3 Use of effective risk management in cloud computing projects

The results have demonstrated that the companies face a number of risks in the implementation of cloud computing projects. In response to such risks however, most companies have always taken the initial step of developing a policy for management and control of such risks associated with cloud computing projects. This response affirms DavoudJolfaie et al. (2015) argument who had stated that many global firms in the current society include rules and policies that regulate their governance systems for cloud computing projects. The rules adopted in this case prevent and control loss of critical data and improve the reliability of the cloud computing procedures and applications. Both the literature and the respondents also indicated that there are also firms that include data encryption methods to prevent and control security problems in their cloud computing applications. It was clear from both the respondents and literature that cloud computing promotes CSP incompatibility problems, increase privacy and confidentially control problems and may also lead to the firm poor data integrity systems.

Results have also shown that companies which have adopted cloud computing practices in project management operations always include a number of security issues. Some of these security issues identified include multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, loss of monitoring and availability, as well as trust management. Backe& Linden (2015) also identified a number of security solutions that can be adopted by such companies including, security models, auditing, policies, SecCloud, RAID, biometrics, self-destructing data, and service hardware when the virtual or physical hardware is needed.

As reported by the respondents, companies can also block/monitor unproductive website browsing, acquire corporate anti-virus software for detection of any form of intrusion or install

firewall that prevent and control all forms of malicious attacks. The antivirus software in this case can be effective in protecting the servers, PCs, Gateways, plus some other things which are vulnerable to attack by malicious users.

Results from the perticipants have indicated that companies have put in place effective systems for managing risks associated with cloud computing projects. For instance, some companies have well managed infrastructure which constantly monitor the systems while others have installed system that create privacy and security both from insiders and third parties of the organization. Some companies have always employed security team that monitor all the outside hackers or people or links trying to enter their domain and block them. One respondent from the study indicated that they always detects unpermitted intruders who pose risks to the organization and also rapidly develop and deploy innovative cloud-native applications designed for the cloud economy.

Results from the respondents have however shown that as the company continues to implement effective risk management in cloud computing projects, they face a number of barriers. The barriers highlighted in this case comprised of lack of experienced team, unexpected threats, budgetary issues, recurrent software attacks by viruses introduced by employees connecting gadgets to company computers, inefficiency to carry out regular updates of antivirus, and constant change of IT setup based on the requirements of the business.

In order to effectively handle the risks associated with cloud computing as well as the barriers related to the same, it has been recommended from the study results that companies should have strategic planning and execution of the same plans, have regular backups and restoration mechanism and continuously update their software and antivirus to avoid the system patches. Companies should also take the necessary steps to secure the data and servers available

in the company domain and ensure security features are up to date so as to be effective in preventing attacks by malware.

CONCLUSION AND RECOMMENDATIONS

6.1 Conclusion

In their adoption of cloud computing systems, there are a number of risks that companies are likely to face. The main security risks experienced by companies are related to data separation, user access control, secure stored data, secure software interfaces, and secure data transfer. The other security concern is that associated with sharing of computer resources by many organizations. Within a virtualized environment in which numerous virtual servers are all hosted within one physical host computer, there exist a risk for access privileges to some other virtual machine to be offered in error, leading to a loss in the confidentiality in data and most likely an exposure to relevant information. Such security risks impact very negatively on the operation of the company as it results into loss of data, finance and important information including company resources. The malicious activities of an insider could potentially have an impact on: the confidentiality, integrity and availability of all kind of data, IP, all kind of services and therefore indirectly on the organization's reputation, customer trust and the experiences of employees.

Most companies have always responded to these risks by coming up with policies for their control and management. Companies which have adopted cloud computing practices have also implemented a number of security risk protection mechanisms such as multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, as well as trust management. Companies can also block/monitor unproductive website browsing, acquire corporate anti-virus software for detection of any form of intrusion or install firewall that prevent and control all forms of malicious attacks. The antivirus software in this case can be effective in protecting the servers, PCs, Gateways, plus some other things which

are vulnerable to attack by malicious users. Moreover, some companies have well managed infrastructure which constantly monitor the systems while others have installed system that create privacy and security both from insiders and third parties of the organization.

For the companies to effectively handle the risks that are associated with cloud computing, it is recommended that companies should have strategic planning and execution of the same plans, have regular backups and restoration mechanism and continuously update their software and antivirus to avoid the system patches.

6.2 Recommendations for future further study

As study was being done, a number of aspects were not covered due to limited resources and time. Moreover, the study only involved 10 participants who were reached out through survey monkey. The small sample size in this case was informed based on the financial and time constrain faced by the researcher. Therefore, it is suggested that future further studies are carried out using a larger sample size to determine the main risks associated with cloud computing projects and establish the use of effective risk management in cloud computing projects. Further studies that involve multiple data collection tools that include interviews, focus group discussion and systematic review of literature are also recommended, paying close focus on the use of effective risk management in cloud computing projects.

References

Adhariani, D., Sciulli, N. and Clift, R. (2017). Research Methodology. In *Financial Management and Corporate Governance from the Feminist Ethics of Care Perspective* (pp. 81-117). Springer International Publishing.

Backe, A., & Linden, H. (2015). Cloud Computing Security: A Systematic Literature Review. *Department of informatics and media: Uppsala University*, 1-50.

Batista, B. G., Estrella, J. C., Ferreira, C. G., Filho, D. L., Nakamura, L. V., Reiff-Marganiec, S., & ... Santana, R. C. (2015). Performance Evaluation of Resource Management in Cloud Computing Environments.*Plos ONE*, *10*(10), 1-21.

Bildosola, I., Río-Belver, R., Cilleruelo, E., &Garechana, G. (2015). Design and Implementation of a Cloud Computing Adoption Decision Tool: Generating a Cloud Road. *Plos ONE*, *10*(7), 1-20.

Caillaud, E., Rose, B., & Goepp, V. (2016). Research methodology for systems engineering: some recommendations. *IFAC-PapersOnLine*, *49*(12), 1567-1572.

Carcary, M., Doherty, E., Conway, G., & McLaughlin, S. (2014). Cloud Computing Adoption Readiness and Benefits Realization in Irish SMEs—An Exploratory Study.*Information Systems Management*, *31*(4), 313-327.

Chang, V., Walters, R. J., & Wills, G. B. (2016).Organizational sustainability modeling-An emerging service and analytics model for evaluating Cloud Computing adoption with two case studies.*International Journal of Information Management*, *36*(1), 167-179.

Charlebois, K., Palmour, N., &Knoppers, B. M. (2016). The Adoption of Cloud Computing in the Field of Genomics Research: The Influence of Ethical and Legal Issues. *PLoS ONE, 11*(10), 1-33.

Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on* (Vol. 1, pp. 647-651). IEEE.

'Cochrane Handbook for Systematic Reviews of Interventions' 2008, *M2presswire*, Newspaper Source, EBSCO*host*.

Creswell, J W. (2013). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, London, Sage.

DavoudJolfaie, S. A., Zadeh, A. R., Rashki, M., &Hemmat, Z. (2015). Cloudy Spine Meta-System Proposed Model in Small Businesses Process Management. *International Journal of Management, Accounting & Economics*, *2*(7), 766-779.

Doorn, N (2010). 'Applying Rawlsian Approaches to Resolve Ethical Issues: Inventory and Setting of a Research Agenda', *Journal Of Business Ethics*, 91, 1, pp. 127-143.

Ferguson-Boucher, K., &Convery, N. (2011).Storing Information in the Cloud – A Research Project.*Journal of the Society of Archivists*, *32*(2), 221-239.

Gonzalez, M. D., & Smith Jr., M. L. (2014). Are Cloud Computing Services Adoption Trends Changing?*Franklin Business & Law Journal*, *2014*(3), 120-144.

Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., & Pourzandi, M. (2012). A quantitative analysis of current security concerns and solutions for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *1*(1), 11.

Griebel, L., Prokosch, H., Köpcke, F., Toddenroth, D., Christoph, J., Leb, I., &Sedlmayr, M. (2015).A scoping review of cloud computing in healthcare.*BMC Medical Informatics & Decision Making*, *15*(1), 1-16.

Gysels, M, Evans, C, Lewis, P, Speck, P, Benalia, H, Preston, N, Grande, G, Short, V, Owen-Jones, E, Todd, C, & Higginson, I. (2013). 'MORECare research methods guidance development: recommendations for ethical issues in palliative and end-of-life care

Gysels, M, Evans, C, Lewis, P, Speck, P, Benalia, H, Preston, N, Grande, G, Short, V, Owen-Jones, E, Todd, C, & Higginson, I. (2013). 'MORECare research methods guidance development: recommendations for ethical issues in palliative and end-of-life care

Han, Y. (2011). Cloud Computing: Case Studies and Total Costs of Ownership. *Information*

Khanagha, S., Volberda, H., Sidhu, J., &Oshri, I. (2013). Management Innovation and Adoption of Emerging Technologies: The Case of Cloud Computing. *European Management Review*, *10*(1), 51-67.

Khorshed, M. T., Ali, A. S., & Wasimi, S. A. (2012). A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. *Future Generation computer systems*, *28*(6), 833-851.

Lee, K. (2012). Security threats in cloud computing environments. *International Journal of Security and Its Applications*, *6*(4), 25-32.

Marković, D. S., Branović, I., &Popović, R. (2014).Review of Cloud Computing In Business.*Singidunum Journal of Applied Sciences*, 673-677.

McCusker, K, & Gunaydin, S. (2014). 'Research using qualitative, quantitative or mixed methods and choice based on the research'.

Nicoletti, B. (2012). Project Management and Cloud Computing. *PM World Today*, *14*(1), 1-11.

Ray, D. (2016). Cloud Adoption Decisions: Benefitting from an Integrated Perspective. *Electronic Journal of Information Systems Evaluation*, *19*(1), 3-22.

Retrieved from https://www.ibm.com/blogs/cloud-computing/2014/01/cloud-computing-defined-characteristics-service-levels/

Royston, S. (2016). How cloud computing changes the way projects are delivered. *TCE: The Chemical Engineer*, 16-17.

Ryan, L. V., & Buchholtz, A. K. (2001). Trust, Risk, and Shareholder Decision Making: An Investor Perspective on Corporate Governance. *Business Ethics Quarterly*, *11*(1), 177-193. Risk Governance (2013). Retrieved from http://www.bnm.gov.my/guidelines/01_banking/04_prudential_stds/gl_013_5.pdf

Schouten, Edwin (2014). Cloud Computing Defined: Characteristics and Service Levels.

Shahzad, A., Golamdin, A. G., & Ismail, N. A. (2016).Opportunity and Challenges using the Cloud Computing in the Case of Malaysian Higher Education Institutions.*International Journal of Management Science & Technology Information*, (20), 1-18.

Singh, S., &Chana, I. (2015).QoS-Aware Autonomic Resource Management in Cloud Computing: A Systematic Review. *ACM Computing Surveys, 48*(3), 42:1-42:46.

Stieninger, M., &Nedbal, D. (2014). Characteristics of Cloud Computing in the Business Context: A Systematic Literature Review. *Global Journal of Flexible Systems Management, 15*(1), 59-68.

Wang, C., Wood, L. C., Abdul-Rahman, H., & Lee, Y. T. (2016).When traditional information technology project managers encounter the Cloud: Opportunities and Dilemmas in the transition to cloud services.*International Journal of Project Management, 34*(3), 371-388.

Watzlawik, M, & Born, A. (2007). *Capturing Identity : Quantitative And Qualitative Methods*, n.p.: University Press of America, Book Index with Reviews, EBSCO*host*, viewed 14 March 2017.

Willett, M., & Von Solms, R. (2014). Cloud-based Email Adoption at Higher Education Institutions in South Africa. *Journal Of International Technology & Information Management, 23*(2), 17-29.

Wilson, V. (2013). 'Research Methods: Mixed Methods Research', *Evidence Based Library & Information Practice*, 8, 2, pp. 275-277, Library, Information Science & Technology Abstracts, EBSCO*host*.

Wilson, V. (2013). 'Research Methods: Mixed Methods Research', *Evidence Based Library & Information Practice*, 8, 2, pp. 275-277, Library, Information Science & Technology Abstracts, EBSCO*host*.

Wisdom, J, Cavaleri, M, Onwuegbuzie, A, & Green, C. (2012). 'Methodological reporting in qualitative, quantitative, and mixed methods health services research articles', *Health Services Research*, 47, 2, pp. 721-745, MEDLINE, EBSCO*host*.

Wisdom, J, Cavaleri, M, Onwuegbuzie, A, & Green, C. (2012). 'Methodological reporting in qualitative, quantitative, and mixed methods health services research articles', *Health Services Research*, 47, 2, pp. 721-745, MEDLINE, EBSCO*host*.

Yang, L., & Huang, C. (2016). Information platform to improve technological innovation capabilities: the role of the cloud platform. *Journal of Civil Engineering & Management*, *22*(7), 936-943.

Yin, R.K.(2013). *Case Study Research: Design and Methods.* 5th edition. London, Sage

Zimara, Sabrina (2013). The Five Essential Characteristics of Cloud Computing. Retrieved from http://erpbloggers.com/2013/07/the-five-essential-characteristics-of-cloud-computing/

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

APPENDIX 1: QUESTIONNAIRE

The Use of Effective Risk Management in Cloud Computing Projects

1. Date of interview ___/__/ 2017 2. Interviewer's initials _____

3. Questionnaire no. _____ 4. Respondents No. _____

SECTION ONE: SOCIO-DEMOGRAPHIC INFORMATION

(Circle the correct answer/fill in space provided)

1.1	Age of the respondent	Years…….	
1.2	What is your highest level of education	1) No formal education 2) Primary school 3) Secondary school 4) College and above	
1.3	What is your marital status?	1) Married 2) Single 3) Cohabiting 4) Divorced 5) Widow	
1.4	What is your gender?	1) Male	

		2) Female	
1.5	Role in the company	Role (designation)…….	

SECTION TWO: SECURITY RISKS IN CLOUD COMPUTING PROJECTS

2.1	Does your organization implement Cloud Computing Projects?	1) Yes 2) No	
2.2	Does your organization experience any security risks in its Cloud Computing Projects?	1) Yes 2) No	
2.3	If yes in 2.2 above, what are the security risks in cloud computing projects that the company is facing?	1) Technical risks 2) Financial risks 3) Compliance/legal risks 4) Security risks 5) Others (mention……..)	
2.4	To what extend does the above risks impact on the organizational operations?	1) Less extend 2) Greater extend 3) No extend 4) No association	
2.5	How do you consider administration's seriousness regarding security risks associated with cloud computing projects?	1) Very serious 2) Less serious 3) Serious 4) Not serious	

SECTION 3: EFFECTIVE RISK MANAGEMENT IN CLOUD COMPUTING PROJECTS

3.1	Does there exists a policy which control risks associated to cloud computing projects?	1) Yes 2) No	
3.2	Does the organization have proper system for management of multi-tenancy and virtualization, data integrity and privacy, denial of service, de-duplication, user access control, backup issues, loss of monitoring and availability, as well as trust management?	1) Yes 2) No	
3.3	Do you block/monitor unproductive web browsing	1) Yes 2) No	
3.4	Does the company has corporate anti-virus software?	1) Yes 2) No	

3.5	What does your antivirus software protect?	PCs Servers Gateways All	
3.6	Has the company installed a system for detecting intrusion	1) Yes 2) No	
3.7	Explain how the installed system is effective in managing risks associated to cloud computing projects in your company	…… …….. ……. ……	
3.8	Does the organization have an installed firewall?	1) Yes 2) No	
3.9	What are some of the main barriers experienced by the company in effective risk management in cloud computing projects	Barriers……. …….. …… ……	
3.10	What do you recommend the organization to do in order to ensure effective risk management in cloud computing projects		

Thank you very much for your time